UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/819,359	03/28/2001	Satoshi Hada	JP919990280US1	3306

7590 10/20/2004

IBM CORPORATION
INTELLECTUAL PROPERTY LAW DEPT.
P.O. BOX 218
YORKTOWN HEIGHTS, NY 10598

EXAMINER	
POLTORAK, PIOTR	

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/819,359	HADA, SATOSHI	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☒ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 have been examined.

Priority

2. Foreign priority has been claimed in this application.

   Acknowledgment is made of applicant's claim for foreign priority based on a Japanese application filed on 3/31/2000. It is noted, however, that applicant has not filed an original and certified copy of the 2000-099867 application as required by 35 U.S.C. 119(b).

   The effective priority date for the subject matter in the pending claims in this application once the paper has been received will be 3/31/2000.

Claim Objections

3. Claims 1, 7-10 and 12 use notation "C" to identify two different functions. For the clarity of the following steps where "C" is used the applicant is advised to change the notation in order to differentiate these two functions; use "**C'** " *(not the " ' " behind the C)* for one and "**C** " for another one for example.
4. Claim 11 is objected to under 37 CFR 1.75(c) as being in improper form because a multiple dependent claim should refer to other claims in the alternative and cannot depend from any other multiple dependent claim. See MPEP § 608.01(n). Accordingly, claim 11 has not been further treated on the merits.
5. Claim 15 is objected to as being dependent on claim 11 and has also not been further treated on the merits.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-10, 14-17 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter.

7. The limitation of claim 1 (pg. 33 line 28 – pg. 2 line 3) is not clear. The cited limitations (pg. 33 line 25-27) suggests that "Z" may or may not be transferred to the verifier computer but the verifier is expected to consider the variable while calculating the function "A=J (v, Y, g, Z)".

   For further consideration the examiner assumes that "and" on pg. 33 line 29 is meant to be "or".

8. Claims 8 and 10 have the same ambiguity; therefore claims 8 and 10 are similarly rejected.

   For further consideration the examiner considers that "and" in claims 8 *(pg. 36 line 28)* and 10 *(pg. 38 line28)* is meant to be "or". As a result, the phrase "are established at the same time" on pg. 36 line 29 and on pg. 38 lines 29-30 is ignored.

9. The word "should" used in claims 1, 7-10 and 12 is ambiguous. It is not clear whether the limitation following "should" is a requirement or, whether it is an option.

10. The limitations starting with "should" are also present in claims 8 and 10; therefore claims 8 and 10 are similarly rejected.

11. Claim 13 recites the limitation as follows: "... for causing a computer to effect the apparatus of claim 9." The meaning of "effect" is not clear.

12. The similar problem exists in claims 14-17; therefore claims 14-17 are similarly rejected.

13. Claims 2-6 are rejected by virtue of their dependence.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 1-10, 12-14 and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Schneier (Bruce Schneier, "Applied Cryptography, Protocols, Algorithms and Source Code in C", 2nd edition, 1996 ISBN: 0471128457)* in view of *Trostle (U.S. Patent No. 6718467).*

15. *Schneier* teaches *Diffie-Helman's* key-exchange algorithm *(pg. 513)* which covers the limitation of claim 1 reading on calculating

Prover (Alice)	*Verifier (Bob)*
A = F(g, a)	
	B = F(g, b)
F (B, a)	X= F (A,b)

16. *Schneier* teaches that F(Y,x) = FX(X,y). He also teaches *Schnorr's* authentication protocol which reads on the limitation of claim 1 disclosed on pg. 1 lines 23 – pg. 2 line 3, in which data required for verifying the equation is sent to the opposite communication party. In addition *Schneier* teaches ciphertext-only cryptanalysis attacks *(pg. 5 last § – pg. 6 first §)*.

17. *Schneier* teaches implicitly that computers are used to implement the algorithms *(pg. 22 and 23, The Purpose of Protocols and The Players sections)*.

18. *Schneier* does not teach transmitting X for verification and determining whether X=F(B,a), and does not teach determining that said relation between the prover computer and the verifier computer is correct.

19. *Trostle* teaches mutual authentication *(col. 7 lines 19-33)*.

20. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend the *Diffie-Hellman's* algorithm by transmitting X for verification, and determining whether X=F(B,a) is established. One of ordinary skill in the art would have been motivated to perform such a modification in order to prevent ciphertext-only attacks.

21. It would also have been obvious to one of ordinary skill in the art to repeat step 1 *("extended" Diffie-Helman's algorithm as cited above; however, this time in regard to the second communicating party, which would read on limitations of claim 1 cited on pg.1 line 20-pg. 2 line 3)* or adding *Schneier's* verification method in order to determine that the relation between the prover computer and verifier computer is correct. One of ordinary skill in the art

would have been motivated to perform such a modification in order to validate communicating parties to lower security risks.

22. *Schnorr's* authentication scheme as presented by *Schneier (last § pg.510 – § 3 pg. 511)* reads on the limitations of claims 2-6.

23. Claims 7-10, 11-14 and 16-17 are substantially equivalent to claims 1-7; therefore claims 7-10, 12-14 and 16-17 are similarly rejected.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571-272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Signature

10/15/04
Date

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100